SC MEDIA

- SC US
- SC UK

Show Search Bar

Search SC Media   Search

- News ⌄
  -
    - Opinions
    - SC Fast Facts
    - SC Reboot Awards 2017
    - Corporate News
    - Dec/Jan Reboot 2017
    - SC Awards Finalists 2018
- Cybercrime ⌄
  - Ransomware
  - Data breaches
  - APTs/Cyberespionage
  - Malware
  - Phishing
  - Insider Threats
  - Cryptocurrency
- Network Security ⌄
  - Mobile Security
  - Cloud Security
  - Privacy & compliance
  - Vulnerabilities
  - IoT
  - Email Security
  - Government/Defense
- Product Reviews ⌄
  - Group Tests
  - First Looks
  - About product reviews
  - Emerging Products
- In Depth ⌄
  - Features
  - Video
  - In Depth
  - SC Magazine Archive
  - SC Reboot Awards 2017
  - Dec./Jan. Reboot 2017
- Events ⌄
  - RiskSec Conference NY
  - Virtual Conferences
  - Webcasts
  - SC Awards 2018
- Whitepapers

- Log in
- ●
- Register

The Cybersecurity source

by Doug Olenick, Online Editor

Follow @DougOlenick

November 15, 2017

Forever 21 reports data breach, failed to turn on POS encryption

- f
- y

- **in**
- **G+**
- **reddit**
- **comment**
- **print**

Clothing retailer Forever 21 reported yesterday that there was unauthorized access of its payment card system when the encryption installed on some of those systems was not operational.

The Los Angeles-based chain said in a [statement](#) that it was informed of the problem by a third-party vendor and that the issue took place between March and October 2017. The 600-store chain noted that only a limited number of point-of-sale payment systems were affected, although the company did not issue say how many could be involved. The retailer had rolled an encryption and tokenization solution to secure its POS stations in 2015, but for an as yet unstated reason this was not in operation in all of its locations.

"Because the investigation is continuing, complete findings are not available, and it is too early to provide further details on the investigation. Forever 21 expects to provide an additional notice as it gets further clarity on the specific stores and timeframes that may have been involved," the company said.

The fact that encryption was turned off on some of the company's payment card readers is indicative of poor cybersecurity hygiene, said Mike Kail, CTO of Cybric.

"Surprised and disappointed to hear this as it sounds like they weren't (fully) PCI compliant. That is the first issue that they should disclose and whomever performed the audit should be held accountable. This continued poor hygiene needs to end."

This revelation comes at a particularly bad time as U.S. retailers are gearing up for Black Friday and the holiday shopping season. Frances Zelazny, VP of behavioral biometrics at BioCatch, recommended that retailers redouble their vigilance when it comes to protecting their POS systems and to be very careful to make sure any security updates received via email are legitimate and not a phishing scheme.

- **f**
- **twitter**
- **in**
- **G+**
- **reddit**
- **comment**
- **print**

Topics:

- [Credit Card](#)
- [Data Breach](#)
- [Retail](#)

You must be a registered member of SC Media US to post a comment.
[Click here to login](#)　|　[Click here to register](#)

Related Articles

[Sonic Drive-In latest to be hit in POS data breach](#)

BY [Doug Olenick](#) Sep 27, 2017

[Hilton to pay $700,000 in data breach settlement with New York, Vermont](#)

BY [Bradley Barth](#) Nov 1, 2017

[Hyatt Hotels reports POS data breach](#)

BY [Doug Olenick](#) Oct 12, 2017

[Data breach exposes about 4 million Time Warner Cable customer records](#)

BY [Doug Olenick](#) Sep 5, 2017

[Chipotle data breach leads to illegal ATM withdrawal](#)

BY [Doug Olenick](#) Jul 21, 2017

Identifying tomorrow's threats

PARTNER CONTENT POWERED BY SCYTHE

The essentials to a modern cloud archive

PARTNER CONTENT POWERED BY MIMECAST

Four bad archiving habits to break

PARTNER CONTENT POWERED BY MIMECAST

A new level of preparedness

PARTNER CONTENT POWERED BY MIMECAST

Techscape is SC Media's content marketing platform. Industry experts share their views in the following categories

Partner Content is sponsored content brought to you by a vendor

USER CENTER

About

Contact

Advisory Board

Meet the team

Subscribe

Editorial Calendar

Executive Insight
submissions

**PRODUCT
REVIEWS**

About/Contact

FAQ

Reprints

OTHER

Privacy Policy

Terms & Conditions

MORE SC SITES

SC Media arms cybersecurity
professionals with the in-depth, unbiased
business and technical information they
need to tackle the countless security
challenges they face and establish risk
management and compliance postures
that underpin overall business strategies.

Follow SC Media

f   🐦   G+